

ABSTRACT OF THE DISCLOSURE

An encrypted-data decrypting apparatus that provides enhanced security protection for programs and data while they are in the processes of decryption to execution after having
5 been encrypted. When a decrypted partial program needs to be loaded into the shared memory M, the controlling unit 11 loads it into an area indicated by the memory location information. According to the memory location information, a plurality of partial programs are sequentially loaded into an area so that
10 one partial program gets overwritten by another; therefore, none of the partial programs exists in the memory for a long time, and thus there is less possibility of having the partial programs referred to illegitimately. In addition, since every time some data is decrypted, the decryption support program authenticating
15 unit 13 confirms authenticity of the decryption support program P, it is possible to prevent having illegitimate references in which the decryption support program is abused.